Mengapa drive USB masih relevan saat ini?

#KingstonIsWithYou

Mengapa drive USB masih relevan saat ini?

Kata pengantar dan konten

Di era digital saat ini, 60% dari semua data perusahaan global disimpan di cloud[1], membahas relevansi teknologi penyimpanan yang mendekati usia tiga puluh tahun mungkin tampak sedikit aneh. Namun, sejak diperkenalkan, pokok penyimpanan ini telah berkembang dan terus berkembang.

Dahulu drive USB hanyalah sarana standar untuk menghubungkan file, drive, dan aplikasi. Solusi saat ini tidak hanya membanggakan kecepatan transfer yang jauh lebih baik, tetapi juga menyediakan media portabel yang andal dan aman merupakan keharusan dalam berbagai situasi. Namun, bagaimana bisa drive USB masih relevan, saat solusi penyimpanan cloud tampaknya telah menawarkan banyak manfaat yang sama?

Dalam eBook ini, kita akan membahas flash drive USB yang berada di tengah lanskap yang didominasi cloud. Didukung oleh wawasan utama dari beberapa pakar industri terkemuka, kami akan mengeksplorasi bagaimana organisasi saat ini masih menggunakan drive USB dan memperdebatkan posisi mereka di antara enkripsi berbasis perangkat lunak, lingkungan penyimpanan independen, dan keamanan data titik akhir.

Mengapa drive USB masih relevan saat ini?

Kontributor

eBook ini disusun bersama tiga pakar TI dan teknologi baru.

Rafael Bloom

Rafael menghabiskan kariernya sebagai senior di bidang Produk Teknologi, Komunikasi Pemasaran, dan Pengembangan Bisnis. Praktik nasihatnya berfokus pada tantangan baru dari perubahan teknologi dan regulasi terhadap organisasi, produk, dan komunikasi. Pekerjaan yang sangat beragam ini membutuhkan keahlian khusus di bidang pengelolaan informasi dan kepatuhan oleh desain, privasi data, dan teknologi baru seperti AdTech, Mobile dan 5G, Kecerdasan Buatan, dan Pembelajaran Mesin.

Tomasz Surdyk

Dengan 24 tahun lebih pengalaman di bidang keamanan TI di dalam pemerintahan, Tomasz adalah tokoh terkemuka ketika menyangkut keamanan informasi, data pribadi, dan keamanan siber. Dahulu, ia telah memeriksa sistem dan jaringan TIK yang memproses informasi rahasia dan data pribadi dalam administrasi pemerintah dan memiliki izin keamanan untuk NATO dan UE. Selama beberapa tahun, Tomasz adalah pemilik perusahaan yang berspesialisasi dalam implementasi solusi aman untuk meningkatkan keamanan informasi bisnis dan data pribadi.

David Clarke

David merupakan satu dari 10 influencer terbaik menurut Thompson Reuter dalam "30 pemimpin pemikiran dan pemikir paling berpengaruh di media sosial, manajemen risiko, kepatuhan, dan teknologi regulasi di Inggris", serta masuk dalam daftar 50 Ahli Global oleh Kingston Technology. Sebelumnya, David memegang beberapa posisi manajemen keamanan seperti Kepala Pengiriman Layanan Keamanan Global dan Kepala Infrastruktur Keamanan untuk 100 perusahaan FTSE Global.

Munculnya flash drive USB

Ketika drive Universal Serial Bus (USB) pertama muncul di pasar lebih dari dua puluh tahun yang lalu, kompatibilitas kolektifnya mengubah permainan di bidang teknologi komputer. Dengan kapabilitas untuk membuat operasi beberapa perangkat dapat diakses secara luas oleh massa, USB segera berevolusi, menawarkan transfer data yang jauh lebih cepat, port USB 3.0, dan bahkan kapabilitas yang lebih besar lagi yang menyertai rilis USB flash drive pertama pada tahun 2000.

Sejak itu, teknologi telah berkembang pesat dalam hal penyimpanan data seluler dan kebutuhan keamanan. Fokusnya ialah pada drive USB generasi sekarang yang dirancang dengan mempertimbangkan kasus penggunaan yang sangat spesifik. Dari perspektif perusahaan, peningkatan pekerjaan jarak jauh dan hibrid, penggunaan layanan cloud, dan masalah keamanan siber mendorong kebutuhan akan solusi yang lebih efektif. Bersamaan ini, persyaratan peraturan menuntut bahwa data perlu disimpan dengan cara yang tepat. Tekanan ini sering diperparah oleh sistem terdistribusi dan kompleks yang dapat berjalan "on-premise" dan di cloud.

Kemudian ada masalah meningkatnya volume data terstruktur dan tidak terstruktur, seperti dokumen, email, foto, video, dan metadata – semuanya menambah kompleksitas kebutuhan penyimpanan perusahaan yang terus berkembang.

Namun, jika penyimpanan cloud dapat menjawab berbagai tantangan ini, relevansi apa yang dimiliki drive USB dalam lanskap bisnis saat ini?

> **Banyak orang menganggap drive USB itu kuno atau sepele karena penggunaannya di masa lalu sebagai perangkat sekali pakai, berkinerja rendah, dan keamanan rendah. - Rafael Bloom**

Penyimpanan portabel yang memenuhi permintaan yang terus berkembang

Sementara pola lama penggunaan drive USB sebagai sarana untuk penyimpanan portabel telah memudar, penggunaan drive USB berkinerja tinggi telah muncul untuk cadangan lokal dan pribadi yang aman dengan lapisan perlindungan dan kerahasiaan data tambahan. Ini dapat menjadi sangat penting bagi data sensitif kepatuhan seperti catatan SDM, data keuangan, catatan perawatan kesehatan, pengamanan kekayaan intelektual (IP), dan semua informasi pengenal pribadi (PII). Selain itu, perangkat generasi ini hadir dengan transfer data yang cepat, penyimpanan, pencadangan, dan kemampuan keamanan yang dapat digunakan untuk:

- Informasi peraturan yang perlu disampaikan langsung
- Surat-surat Hukum dan Keuangan yang perlu dikirimkan dan dicetak di tempat atau di luar
- Setiap lingkungan yang berpotensi tidak bersahabat tempat Ransomware dapat menjadi ancaman
- Mentransfer ke sistem pencetakan di mana akses jaringan tidak diperbolehkan

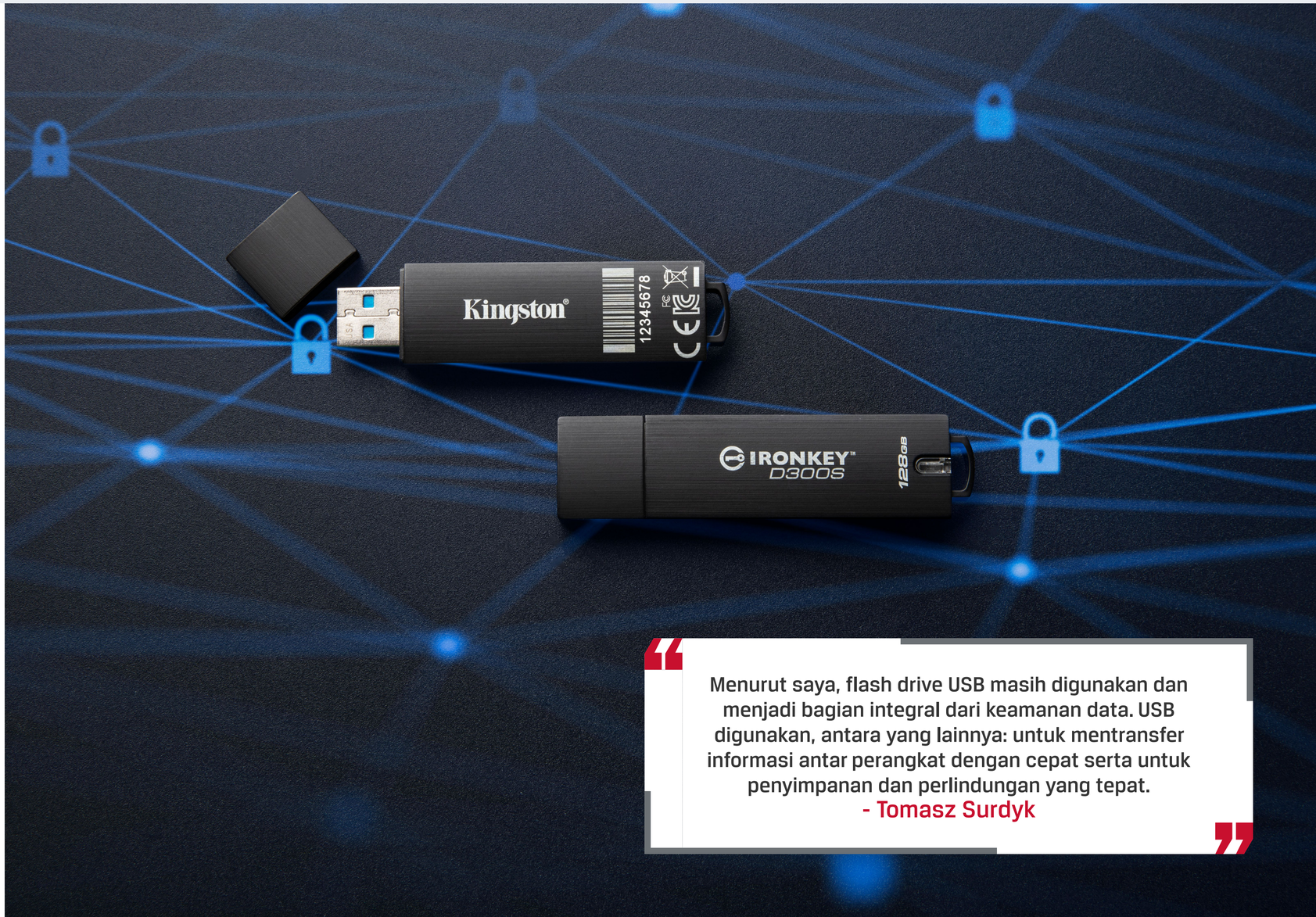
Penyedia USB terenkripsi terkemuka, Kingston Technology, telah mengikuti perkembangan permintaan dengan merilis solusi seperti Kingston IronKey™ S1000. Drive USB terenkripsi yang terbaik di kelasnya ini memenuhi standar paling ketat dengan kemampuan untuk melindungi data rahasia dengan menyediakan enkripsi 256-bit XTS-AES disertai dengan cryptochip terpisah yang memiliki perlindungan anti-gangguan yang kuat. Selain itu, FIPS 140-2 Level 3 Bersertifikat. Ini artinya telah divalidasi secara resmi oleh pemerintah AS untuk efektivitas sebagai bagian dari perangkat keras kriptografi, menjadikannya ideal untuk organisasi yang membutuhkan ketenangan pikiran lebih dalam hal perlindungan data.

Drive USB terenkripsi perangkat keras tersebut menawarkan solusi manajemen perangkat aman yang terpusat, baik datanya berbasis cloud atau on-premise. Penyimpanan data terenkripsi yang sesuai dan mudah digunakan tanpa memerlukan perangkat lunak serta menghemat waktu TI yang berharga, menawarkan solusi yang dirancang untuk penyebaran yang cepat dan efisien.

Penyimpanan portabel yang memenuhi permintaan yang terus berkembang

Pencadangan dan pengarsipan adalah contoh lain di mana drive USB dapat digunakan untuk melindungi aset digital dalam jangka panjang, dan terpisah dari layanan Cloud pihak ketiga. Meskipun benar bahwa transfer data besar mudah ditangani di Cloud, IP berpemilik masih cukup sensitif sehingga selayaknya disimpan di drive USB terenkripsi dan aman, yang dapat disimpan jauh dari internet dan diamankan.

Kemudian, akan selalu ada kondisi di mana organisasi membutuhkan data secara logis dan fisik di bawah kendali mereka, terutama saat menggunakan drive terenkripsi. Selain itu, ada kasus di mana penyimpanan pada HDD/SSD tidak dapat dienkripsi. Menggunakan drive USB terenkripsi eksternal dapat mengatasi masalah ini, seperti: Kingston IronKey D300S. Flash Drive USB ini memiliki enkripsi perangkat keras XTS 256-bit Standar Enskripsi Canggih (AES), yang merupakan jenis cipher blok yang dapat mengenkripsi blok data 128-bit. Saat diperlukan untuk mengenkripsi data di luar ini, AES akan menggunakan mode cipher blok XTS yang mampu memberikan perlindungan data yang lebih baik dan lebih kuat dibandingkan mode sebelumnya.



> Menurut saya, flash drive USB masih digunakan dan menjadi bagian integral dari keamanan data. USB digunakan, antara yang lainnya: untuk mentransfer informasi antar perangkat dengan cepat serta untuk penyimpanan dan perlindungan yang tepat.
> - Tomasz Surdyk

Enkripsi: Berbasis perangkat keras vs berbasis perangkat lunak

Melihat cara data dienkripsi, dapat dikatakan bahwa enkripsi perangkat keras lebih mudah dikelola, dan lebih aman dibandingkan enkripsi perangkat lunak. Ini karena proses enkripsi disimpan terpisah dari sistem host lainnya, sehingga lebih sulit dihalangi untuk atau dihancurkan. Manajemen tingkat perangkat yang terpusat memungkinkan kontrol drive pada LAN dan koneksi Internet, serta merupakan alat yang andal untuk:

- Menetapkan dan menegakkan kebijakan penggunaan USB individu dan/atau grup terenkripsi
- Mengaudit aktivitas file untuk melacak data yang berpindah keluar masuk organisasi Anda dengan lebih baik.
- Menyediakan cadangan konten jarak jauh untuk pemindahan data penting
- Menonaktifkan perangkat dari jarak jauh saat USB hilang atau terganggu
- Melakukan pengaturan ulang kata sandi jarak jauh jika lupa

Jika drive yang diotorisasi dikelola dengan benar dengan cara ini, risiko data sensitif disalin dan dibagikan dapat diminimalkan. Selain itu, drive USB terenkripsi perangkat keras modern menawarkan sejumlah besar fitur keamanan ekstra yang membantu mencegah file dan pesan diakses atau dibaca oleh siapa pun selain penerima yang dituju.

> **Saya percaya bahwa enkripsi perangkat keras lebih baik dibandingkan enkripsi perangkat lunak. Perbedaan antara metode enkripsi perangkat keras dan perangkat lunak signifikan Dalam kasus perangkat terenkripsi perangkat keras, tidak mudah menyerah pada serangan semacam itu. - Tomasz Surdyk**

Enkripsi: Berbasis perangkat keras vs berbasis perangkat lunak

Sementara bisnis mempertimbangkan enkripsi berbasis perangkat lunak karena biaya, ini mungkin sedikit kurang bijaksana. Solusi berbasis perangkat lunak berbagi sumber daya enkripsi perangkat host dengan program lain, sehingga sama amannya dengan komputer dan sering kali memerlukan pembaruan perangkat lunak yang - jika tidak dipelihara - akan membuat Anda rentan. Drive USB yang dienkripsi perangkat lunak dapat menjadi sasaran serangan brute force tak terbatas untuk menebak kata sandi, dan mereka tidak memiliki sarana untuk menahan serangan kamus berbasis perangkat lunak - yang dapat menguji jutaan kombinasi karakter dalam waktu singkat.

Selain itu, enkripsi perangkat lunak juga merupakan enkripsi yang dapat dihapus. Setiap karyawan dengan drive terenkripsi perangkat lunak dapat menyalin data, memformat drive USB, dan enkripsi akan dihapus. Kemudian mereka dapat menyalin kembali file data dan menggunakan drive tanpa repot mengautentikasi pada platform dan OS yang berbeda.

Seperti yang kami katakan sebelumnya, dengan enkripsi berbasis perangkat keras, "enkripsi" fisik - dan penyimpanan data berikutnya - dilakukan secara independen dari sistem host. Ini memastikan lapisan pertahanan ekstra, jika sistem pernah disusupi.

Hal ini tidak dapat diabaikan, terutama bagi mereka yang berada di industri seperti keuangan, perawatan kesehatan, dan pemerintahan. Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) dan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) seringkali memiliki persyaratan ketat terkait enkripsi informasi sensitif.

Mematuhi peraturan ini dengan menggunakan perangkat terenkripsi perangkat keras yang kuat pada akhirnya akan membantu organisasi menghindari denda yang mahal, tuntutan hukum, dan kerusakan reputasi yang berpotensi melemahkan. Sementara drive yang dienkripsi perangkat keras bisa jadi lebih mahal daripada drive USB komoditas yang lebih murah, biaya hukum pelanggaran dapat dengan mudah membayar ratusan drive setara dengan beberapa jam biaya konsultasi hukum.

Meningkatnya kebutuhan untuk melindungi data sensitif

> Enkripsi semua data secepat mungkin, cadangkan menggunakan 321 Metodologi (USB dapat menjadi pilihan karena telah tersedia), dan terapkan kapabilitas segmentasi mikro yang cepat. - David Clarke

Dalam hal melindungi data sensitif dari kehilangan dan pencurian, setiap organisasi memiliki kewajiban untuk memastikan perangkat mereka memiliki fitur keamanan yang memadai. Penting juga untuk dipertimbangkan meskipun ada segudang ancaman dunia maya yang terus berkembang, tingkat kematangan digital dan keterampilan manajemen data titik akhir pengguna tetap menjadi faktor risiko utama jika tidak ditangani. Ancaman orang dalam yang mencakup hilangnya kontrol data atau perangkat penyimpanan USB, transmisi data di luar lingkungan yang aman, penggunaan drive USB yang tidak terenkripsi, dan berbagi kata sandi, semuanya dapat disebabkan oleh kurangnya uji tuntas pengguna akhir. Semua itu dapat dihindari dengan pelatihan, pendidikan, dan solusi drive USB yang tepat.

> Organisasi harus memiliki peta data yang jelas, termasuk tingkat kepentingan dan/atau sensitivitas semua set data, dengan rencana menangani data yang paling penting lebih dulu, baik dengan menghapus koneksi ke data secara fisik atau memutuskan sumber data tersebut. Mampu mengisolasi sistem yang terdampak dengan cepat adalah kuncinya – dan sekali lagi, memiliki rencana terdokumentasi yang telah Anda praktikkan sangatlah penting. - Rafael Bloom

Perencaan awal dan struktur komunikasi yang dipraktikkan dengan baik juga manjadi faktor kunci dalam menghadapi potensi ancaman eksistensial. Ancaman dunia maya saat ini dimaksudkan untuk menargetkan titik lemah organisasi.

Waktu terbaik untuk mengembangkan paket USB terenkripsi adalah sebelum benar-benar dibutuhkan, dengan memasukkan drive dan kebijakan USB terenkripsi ke dalam strategi keamanan keseluruhan organisasi Anda. Tidak memiliki rencana untuk USB terenkripsi dan tidak ada pedoman membuat Anda tidak memiliki apa pun untuk dikembangkan, dan organisasi Anda terbuka untuk risiko di setiap tingkat - termasuk kegagalan untuk mematuhi peraturan, seperti Peraturan Perlindungan Data Umum (GDPR), dengan pasal 32 secara khusus menyatakan bahwa data sensitif perlu dienkripsi.

> Pengguna memproses data sensitif Kehilangan hal ini meningkatkan tanggung jawab dan secara signifikan mempengaruhi citra dan keamanan perusahaan. Untuk melindungi data sensitif, berbagai solusi keamanan harus digunakan, termasuk enkripsi data.
> - Tomasz Surdyk

Mengamankan data keuangan sensitif

Seiring dengan implikasi keamanan, ada juga standar kepatuhan yang harus dipatuhi oleh solusi penyimpanan dan pencadangan data. Beberapa praktik ini, seperti kebutuhan untuk mengelola dan menerapkan jadwal penyimpanan data, adalah hal yang umum di seluruh vertikal di antara yang lainnya, seperti migrasi data perusahaan ke cloud, diperlakukan dengan sangat berbeda.

Di banyak vertikal, seperti layanan keuangan, peraturan yang mewajibkan pengelolaan data yang tepat telah diterapkan. Khususnya bank, pada awalnya sangat enggan menggunakan pihak ketiga untuk penyimpanan dan pencadangan, dan banyak yang masih bersikeras untuk menjadi pemilik semua infrastruktur data mereka.

Lembaga keuangan juga terikat untuk mematuhi daftar peraturan dan standar keamanan data yang terus bertambah, seperti Sarbanes-Oxley Act (SOX) dan Peraturan Perlindungan Data Umum (GDPR). Namun, seiring bertambahnya jumlah karyawan dan kontraktor mobile, risiko kebocoran data dan kegagalan dalam mematuhi mandat yang diberlakukan oleh undang-undang dan standar tersebut juga meningkat.

Sebenarnya, upaya kepatuhan dapat dikompromikan dengan sangat mudah jika karyawan mobile gagal melindungi identitas digital mereka, ruang kerja portabel, catatan pelanggan, dan data keuangan yang mereka bawa. Itulah sebabnya semakin banyak organisasi yang beralih ke solusi keamanan seluler seperti drive USB terenkripsi Kingston IronKey, untuk melindungi identitas dan aplikasi digital ke mana pun karyawan mereka membawanya.

> **Saat Anda mempertimbangkan pergeseran tren keseluruhan ke jejak TI yang lebih terdistribusi dan skalabilitas infrastruktur Cloud, mudah untuk melihat bagaimana sebagian besar industri, dan sebagian besar UKM, tidak lagi berurusan dengan pengelolaan ruang server berpendingin. - Rafael Bloom**

Akses aman ke data kesehatan pasien

Kesehatan adalah industri lain di mana keamanan data lebih penting dari sebelumnya. Informasi pasien bahkan berisiko lebih besar untuk dicuri, dengan pelanggaran yang mengekspos 45,67 juta catatan pasien pada tahun 2021, total tahunan terbesar sejak 2015[2]. Dalam hal penyimpanan dan pencadangan data, data pasien adalah informasi medis yang penting dan komprehensif yang memungkinkan penyedia layanan kesehatan untuk merawat pasien dengan aman.

Ini dapat mencakup semuanya, mulai dari file Catatan Kesehatan Elektronik (EHR) pasien yang berisi riwayat kesehatan, tes, foto, dan gambar radiografi, hingga file administratif termasuk catatan penggajian, asuransi pasien, dan hutang dagang. Dihadapkan dengan tenaga kerja mobile yang berkembang dan pasar perawatan kesehatan global yang sedang mengalami pergolakan dan transformasi besar, tidak heran jika penyedia layanan kesehatan saat ini peduli dengan keamanan data.

> **Khususnya dengan ransomware yang menjadi bagian dari industri yang berkembang, setiap organisasi yang menangani data sensitif harus mempertimbangkan cara beroperasi di bawah tekanan ekstrim. - Rafael Bloom**

Selain itu, kegagalan mengantisipasi risiko dan memenuhi mandat ketat seperti Undang-Undang Probabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) atau Undang-Undang Teknologi Informasi Kesehatan untuk Kesehatan Ekonomi dan Klinis (HITECH) dapat mengakibatkan pelanggaran data perawatan kesehatan yang mahal, yang selanjutnya dapat menggoyahkan kepercayaan pasien, mitra, atau regulator.

Dengan solusi seperti rangkaian drive USB terenkripsi Kingston IronKey, organisasi layanan kesehatan dapat menetapkan kebijakan untuk kata sandi, penggunaan aplikasi, pemulihan, dan lainnya – di beberapa atau ribuan drive, dari satu konsol. Pekerja mobile dan garis depan dapat diberdayakan untuk mendukung lebih banyak pasien, dengan solusi ramah pengguna yang menghilangkan kebutuhan karyawan untuk menginstal driver atau perangkat lunak lain, untuk mengakses data yang tersimpan dengan aman. Sementara pengguna dan administrator dapat dengan mudah dan cepat mengunci data, ke mana pun perginya.

Drive USB di masa depan penyimpanan cloud

> **Penyimpanan data cloud adalah masa kini dan masa depan. Saya masih berpendapat bahwa mengamankan data secara fisik, mis. dengan menggunakan drive USB terenkripsi, adalah yang paling aman. Pengguna tidak memiliki kendali penuh atas apa yang terjadi di cloud. Namun, kami memiliki kendali atas data dalam drive USB terenkripsi, yang kami amankan dan simpan sendiri. Selain dari kami, tidak ada yang memiliki akses ke media ini. - Tomasz Surdyk**

Sekarang setelah manfaat drive USB jelas, apa sebenarnya perannya di masa depan penyimpanan cloud?

Satu dekade yang lalu, drive USB sangat diminati sebagai alat utama untuk menyimpan dan mentransfer data dengan mudah. Namun, dengan dampak model kerja hibrid baru dan tim yang semakin terdistribusi, cloud kini menyediakan akses cepat dan mudah dari banyak perangkat ke informasi yang tersimpan. Sementara flash drive pernah sangat populer karena kemudahan unik yang ditawarkan untuk mengangkut file. Saat ini, layanan penyimpanan cloud menawarkan kemudahan portabilitas file yang lebih besar.

Meskipun demikian, masih banyak batasan dalam hal penyimpanan cloud. Konektivitas jaringan diperlukan, yang tidak hanya menentukan cara dan waktu file dapat dicadangkan atau ditransfer, namun juga menambah urusan keamanan ekstra. Ketika sebuah perusahaan mewajibkan penggunaan cloud, perusahaan belum tentu dapat mengontrol dari mana data diakses. Karenanya, tindakan sederhana mengakses VPN menggunakan koneksi Wi-Fi pribadi atau publik akan membuka risiko diretas. Selain itu, layanan Cloud sangat menarik bagi pelaku ancaman, dengan mayoritas semua malware (61%) sekarang dikirimkan melalui aplikasi cloud[3].

> **Tampak bijaksana untuk mempertimbangkan hal yang terjadi ketika cloud tidak tersedia, skenario tempat data harus tersedia 100%, dan tempat penyimpanan jangka panjang dapat menciptakan kerentanan. - David Clarke**

Drive USB di masa depan penyimpanan cloud

Di sisi lain, enkripsi USB dapat dilakukan baik melalui perangkat keras maupun perangkat lunak. Enkripsi berpusat perangkat keras dan tanpa perangkat lunak adalah cara paling efektif untuk menyediakan perlindungan dari serangan siber. Ini solusi yang sangat baik dan tidak rumit untuk melindungi dari pelanggaran data, serta dapat memenuhi standar kepatuhan yang ketat dengan keamanan tertinggi dalam perlindungan data untuk membantu organisasi mengelola ancaman dan mengurangi risiko dengan percaya diri.

Karena mandiri, drive USB terenkripsi perangkat keras tidak memerlukan elemen perangkat lunak pada komputer host. Dengan meniadakan kerentanan perangkat lunak akan menghilangkan kemungkinan serangan brute force, sniffing, dan hash memori. Drive USB terenkripsi perangkat lunak juga menghadapi risiko setiap pengguna dapat menonaktifkan enkripsi dengan memformat drive di komputer mana pun dan menggunakan drive untuk menyimpan data sensitif dengan cara yang tidak terlindungi.

Drive USB yang dienkripsi perangkat keras juga menawarkan sarana fisik yang luar biasa dalam menjaga keamanan data. Ini memungkinkan kriteria akses informasi untuk ditetapkan oleh pengguna atau admin, dan dapat berintegrasi dengan solusi titik akhir lokal yang ada. Ini menjadikannya solusi yang nyaman dan hemat biaya untuk banyak skenario di mana penyimpanan cloud tidak akan berfungsi, atau tidak akan menjadi solusi yang efektif. Ini mungkin saat data perlu disimpan dari perangkat yang tidak terhubung ke jaringan, yang harus bersifat pribadi, atau memerlukan akses saat offline.

> **Jika kita menganggap data sebagai 'panas' atau 'dingin' tergantung pada tingkat penggunaannya setiap hari untuk suatu organisasi, maka mungkin lebih efisien untuk menyimpan data 'dingin' di cloud dan lebih mengandalkan penyimpanan USB lokal untuk penyimpanan data 'panas', jika kontinuitas operasional dan kinerja tinggi merupakan hal yang lebih penting bagi organisasi, atau bagi fungsi atau proses penting bisnis tertentu. - Rafael Bloom**

Ringkasan

Meskipun kami tidak dapat memprediksi hadirnya inovasi di masa mendatang, hal yang dapat kami tawarkan adalah portofolio drive USB juaara yang menawarkan berbagai solusi terenkripsi dinamis bagi semua tingkat persyaratan perlindungan data seluler. Dari drive USB yang menampilkan keypad alfanumerik untuk perlindungan PIN yang mudah digunakan; untuk sertifikasi FIPS 140-2-Level 3 untuk enkripsi tingkat tertinggi beserta perlindungan anti-gangguan; dengan teknologi SuperSpeed USB 3.1 yang tidak berkompromi pada keamanan, produk Kingston IronKey dirancang untuk memenuhi tantangan data Anda, dengan drive USB yang menjanjikan transportasi data yang kuat dan efektif serta solusi penyimpanan data seluler.

Tim ahli khusus kami siap mendukung Anda di setiap langkah perjalanan penyimpanan data Anda, menawarkan uluran tangan tepercaya dalam membantu menemukan solusi penyimpanan yang tepat untuk memenuhi kebutuhan Anda.

Kami memiliki keterampilan dan kemampuan teknis untuk membantu menjaga keamanan informasi rahasia dan mematuhi peraturan baru, baik Anda ingin membuat paket USB terenkripsi, mengidentifikasi drive USB terbaik untuk bisnis Anda, atau menetapkan dan menerapkan kebijakan keamanan. Menawarkan layanan yang sangat dipersonalisasi, kami berkomitmen untuk memberikan produk yang mendukung prioritas penyimpanan data, memungkinkan Anda untuk mengimbangi kecepatan pergerakan dunia bisnis yang pernah terjadi sebelumnya.

Tentang Kingston

Dengan pengalaman 35 tahun, Kingston memiliki pengetahuan untuk mengidentifikasi dan menyelesaikan tantangan data seluler Anda – memudahkan tenaga kerja untuk bekerja dengan aman tanpa mengorbankan organisasi Anda.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou